

## CLAIMS

1. A method for performing path-sensitive value flow analysis on an abstract program, the abstract program having a plurality of statements that are derived from complex statements coded within a software program, the method comprising:

tracking a concrete state and value alias information for each statement along each relevant path in the abstract program;

storing the concrete state and value alias information for each statement along each relevant path in a symbolic store, the symbolic store storing a plurality of symbolic states, each symbolic state comprising the concrete state at a specific location along a specific relevant path in the abstract program and the value alias information at the specific location along the specific relevant path, the set of aliases being associated with a designated value that is being analyzed;

upon encountering a decisional statement, proceeding individually along each decision path associated with the decisional statement as long as the concrete state in the symbolic state being processed at the decisional statement reflects that the decision path is relevant; and

merging two symbolic states in the symbolic store if the two symbolic states exist for the same specific location in the abstract program and if the value alias information in the two symbolic states are identical.

2. The method of claim 1, wherein the two symbolic states are merged by deleting information in the concrete state of both symbolic states if the information differs between the two symbolic states.

1       3. The method of claim 1, wherein the value alias information is  
2 obtained using imprecise memory alias analysis.

3  
4       4. The method of claim 1, wherein the value alias information includes  
5 a first set of aliases that identify aliases for the designated value and a second set  
6 of aliases that identify possible aliases for the designated value.

7  
8       5. The method of claim 4, wherein the second set of aliases is over-  
9 inclusive.

10  
11      6. The method of claim 4, wherein the first set and second set of aliases  
12 are determined by performing transform functions on the first and second set of  
13 aliases based on a type of statement that is being processed in the abstract  
14 program.

15  
16      7. The method of claim 6, wherein the type of statement includes an  
17 initial statement, the transform functions for the first set of aliases include a  
18 generate transfer function and a remove transfer function, the generate transfer  
19 function adds the variable X to the first set of aliases, the remove transfer function  
20 is the empty set.

21  
22      8. The method of claim 6, wherein the type of statement includes a  
23 scalar assignment in which a variable Y is assigned to a variable X, the transform  
24 functions for the first set of aliases include a generate transfer function and a  
25 remove transfer function, the generate transfer function adds the variable X to the

1 first set if the variable Y was in the first set before the statement and adds a field  
2 pointed to by variable X to the first set if the field dereferenced by variable Y was in  
3 the first set before the statement, the remove transfer function removes fields  
4 referenced by the variable X, and removes the variable X and any field that points  
5 to the same memory location as variable X, if the variable Y was not in the first set  
6 before the statement.

7  
8 9. The method of claim 6, wherein the type of statement includes an  
9 assignment in which an address of variable Y is assigned to a variable X, the  
10 transform functions for the first set of aliases include a generate transfer function  
11 and a remove transfer function, the generate transfer function adds the dereference  
12 of variable X to the first set if the variable Y was in the first set before the  
13 statement, the remove transfer function removes fields referenced with the  
14 variable X, removes the variable X, and removes any field that points to the same  
15 memory location as variable X.

16  
17 10. The method of claim 6, wherein the type of statement includes a call  
18 to a memory allocation function with a return value assigned to a variable X, the  
19 transform functions for the first set of aliases include a generate transfer function  
20 and a remove transfer function, the generate transfer function is an empty set, the  
21 remove transfer function removes fields referenced with the variable X, removes  
22 the variable X, and removes any field that points to the same memory location as  
23 variable X.

1        11. The method of claim 6, wherein the type of statement includes an  
2 assignment in which a field F pointed to by variable Y is assigned to a variable X,  
3 the transform functions for the first set of aliases include a generate transfer  
4 function and a remove transfer function, the generate transfer function adds the  
5 variable X to the first set if the field F pointed to by the variable Y was in the first  
6 set before the statement, the remove transfer function removes fields referenced by  
7 the variable X, and removes the variable X and any field that points to the same  
8 memory location as variable X, if the variable Y was not in the first set before the  
9 statement.

10  
11        12. The method of claim 6, wherein the type of statement includes an  
12 assignment in which an address of a field F referenced by variable Y is assigned to  
13 variable X, the transform functions for the first set of aliases include a generate  
14 transfer function and a remove transfer function, the generate transfer function  
15 adds the dereference of variable X to the first set if the field F referenced by  
16 variable Y was in the first set before the statement, the remove transfer function  
17 removes fields referenced with the variable X, removes the variable X, and  
18 removes any field that points to the same memory location as variable X.

19  
20        13. The method of claim 6, wherein the type of statement includes an  
21 assignment in which a variable Y is assigned to a field F referenced by variable X,  
22 the transform functions for the first set of aliases include a generate transfer  
23 function and a remove transfer function, the generate transfer function adds the  
24 field F referenced by variable X if the variable Y was in the first set before the  
25 statement, the remove transfer function removes any field referenced by a variable

1 Z such that the variable Z refers to the same memory location as the field F  
2 referenced by the variable X, and if the variable Y was not in the first set, removes  
3 the field F referenced by the variable X, any field that points to the same memory  
4 location as the field F referenced by the variable X, and any variable that refers to  
5 the same memory location as the field F referenced by the variable X before the  
6 statement.

7  
8 14. The method of claim 6, wherein the transform functions for the type  
9 of statement include a generate transfer function and a remove transfer function  
10 for determining the first set of aliases, the generate transfer function is the empty  
11 set, the remove transfer function removes any variable that pointed to the same  
12 memory location as a memory cell that was updated by the statement and removes  
13 any field if the memory cell updated by the statement pointed to the same memory  
14 location as the field or the pointer.

15  
16 15. The method of claim 6, wherein the type of statement includes an  
17 initial statement, the transform functions for the second set of aliases include a  
18 generate transfer function and a remove transfer function, the generate transfer  
19 function adds the variable X to the second set of aliases, the remove transfer  
20 function is the empty set.

21  
22 16. The method of claim 6, wherein the type of statement includes a  
23 scalar assignment in which a variable Y is assigned to a variable X, the transform  
24 functions for the second set of aliases include a generate transfer function and a  
25 remove transfer function, the generate transfer function adds the variable X to the

1 second set if the variable Y refers to the same memory location as one of the  
2 aliases in the second set of aliases before the statement, the remove transfer  
3 function removes the variable X.

4

5 17. The method of claim 6, wherein the type of statement includes an  
6 assignment in which an address of variable Y is assigned to a variable X, the  
7 transform functions for the second set of aliases include a generate transfer  
8 function and a remove transfer function, the generate transfer function is the  
9 empty set, the remove transfer function removes the variable X from the second  
10 set.

11

12 18. The method of claim 6, wherein the type of statement includes a call  
13 to a memory allocation function with a return value assigned to a variable X, the  
14 transform functions for the second set of aliases include a generate transfer  
15 function and a remove transfer function, the generate transfer function is the  
16 empty set, the remove transfer function removes the variable X from the second  
17 set.

18

19 19. The method of claim 6, wherein the type of statement includes an  
20 assignment in which a field F pointed to by variable Y is assigned to a variable X,  
21 the transform functions for the second set of aliases include a generate transfer  
22 function and a remove transfer function, the generate transfer function adds the  
23 variable X if the field F pointed to by variable Y refers to the same memory  
24 location as one of the aliases in the second set of aliases before the statement, the  
25 remove transfer function removes the variable X from the second set of aliases.

1  
20. The method of claim 6, wherein the type of statement includes an  
3 assignment in which an address of a field F referenced by variable Y is assigned to  
4 variable X, the transform functions for the second set of aliases include a generate  
5 transfer function and a remove transfer function, the generate transfer function is  
6 the empty set, the remove transfer function removes the variable X from the  
7 second set.

8  
9 21. The method of claim 6, wherein the type of statement includes an  
10 assignment in which a variable Y is assigned to a field F referenced by variable X,  
11 the transform functions for the second set of aliases include a generate transfer  
12 function and a remove transfer function, the generate transfer function adds the  
13 field F referenced by variable X to the second set if the variable Y refers to the  
14 same memory location as one of the aliases in the second set before the statement,  
15 the remove transfer function is the empty set.

16  
17 22. The method of claim 6, wherein the transform functions for the type  
18 of statement include a generate transfer function and a remove transfer function  
19 for determining the second set of aliases, the generate transfer function adds an  
20 expression if the expression was updated by the statement or if one of the memory  
21 locations looked up when executing the statement pointed to a memory location in  
22 the second set of aliases, the remove transfer function is the empty set.

23  
24 23. A computer-readable medium for performing path-sensitive value  
25 flow analysis, comprising:

1 applying transform functions to determine value alias information based on  
2 a type of statement that is being processed in an abstract program, the value alias  
3 information comprising a first set of aliases that identify aliases for a designated  
4 value that is being analyzed and a second set of aliases that identify possible  
5 aliases for the designated value, a portion of the value alias information being  
6 obtained using imprecise memory alias analysis.

7  
8 24. The computer-readable medium of claim 23, wherein the type of  
9 statement includes an initial statement, the transform functions for the first set of  
10 aliases include a generate transfer function and a remove transfer function, the  
11 generate transfer function adds the variable X to the first set of aliases, the remove  
12 transfer function is the empty set.

13  
14 25. The computer-readable medium of claim 23, wherein the type of  
15 statement includes a scalar assignment in which a variable Y is assigned to a  
16 variable X, the transform functions for the first set of aliases include a generate  
17 transfer function and a remove transfer function, the generate transfer function  
18 adds the variable X to the first set if the variable Y was in the first set before the  
19 statement and adds a field pointed to by variable X to the first set if the field  
20 dereferenced by variable Y was in the first set before the statement, the remove  
21 transfer function removes fields referenced by the variable X, and removes the  
22 variable X and any field that points to the same memory location as variable X, if  
23 the variable Y was not in the first set before the statement.

1        26. The computer-readable medium of claim 23, wherein the type of  
2 statement includes an assignment in which an address of variable Y is assigned to  
3 a variable X, the transform functions for the first set of aliases include a generate  
4 transfer function and a remove transfer function, the generate transfer function  
5 adds the dereference of variable X to the first set if the variable Y was in the first  
6 set before the statement, the remove transfer function removes fields referenced  
7 with the variable X, removes the variable X, and removes any field that points to  
8 the same memory location as variable X.

9  
10        27. The computer-readable medium of claim 23, wherein the type of  
11 statement includes a call to a memory allocation function with a return value  
12 assigned to a variable X, the transform functions for the first set of aliases include  
13 a generate transfer function and a remove transfer function, the generate transfer  
14 function is an empty set, the remove transfer function removes fields referenced  
15 with the variable X, removes the variable X, and removes any field that points to  
16 the same memory location as variable X.

17  
18        28. The computer-readable medium of claim 23, wherein the type of  
19 statement includes an assignment in which a field F pointed to by variable Y is  
20 assigned to a variable X, the transform functions for the first set of aliases include  
21 a generate transfer function and a remove transfer function, the generate transfer  
22 function adds the variable X to the first set if the field F pointed to by the variable  
23 Y was in the first set before the statement, the remove transfer function removes  
24 fields referenced by the variable X, and removes the variable X and any field that

25

1 points to the same memory location as variable X, if the variable Y was not in the  
2 first set before the statement.

3  
4 29. The 'computer-readable medium of claim 23, wherein the type of  
5 statement includes an assignment in which an address of a field F referenced by  
6 variable Y is assigned to variable X, the transform functions for the first set of  
7 aliases include a generate transfer function and a remove transfer function, the  
8 generate transfer function adds the dereference of variable X to the first set if the  
9 field F referenced by variable Y was in the first set before the statement, the  
10 remove transfer function removes fields referenced with the variable X, removes  
11 the variable X, and removes any field that points to the same memory location as  
12 variable X.

13  
14 30. The computer-readable medium of claim 23, wherein the type of  
15 statement includes an assignment in which a variable Y is assigned to a field F  
16 referenced by variable X, the transform functions for the first set of aliases include  
17 a generate transfer function and a remove transfer function, the generate transfer  
18 function adds the field F referenced by variable X if the variable Y was in the first  
19 set before the statement, the remove transfer function removes any field referenced  
20 by a variable Z such that the variable Z refers to the same memory location as the  
21 field F referenced by the variable X, and if the variable Y was not in the first set,  
22 removes the field F referenced by the variable X, any field that points to the same  
23 memory location as the field F referenced by the variable X, and any variable that  
24 refers to the same memory location as the field F referenced by the variable X  
25 before the statement.

1  
2       31. The computer-readable medium of claim 23, wherein the transform  
3 functions for the type of statement include a generate transfer function and a  
4 remove transfer function for determining the first set of aliases, the generate  
5 transfer function is the empty set, the remove transfer function removes any  
6 variable that pointed to the same memory location as a memory cell that was  
7 updated by the statement and removes any field if the memory cell updated by the  
8 statement pointed to the same memory location as the field or the pointer.

9  
10      32. The computer-readable medium of claim 23, wherein the type of  
11 statement includes an initial statement, the transform functions for the second set  
12 of aliases include a generate transfer function and a remove transfer function, the  
13 generate transfer function adds the variable X to the second set of aliases, the  
14 remove transfer function is the empty set.

15  
16      33. The computer-readable medium of claim 23, wherein the type of  
17 statement includes a scalar assignment in which a variable Y is assigned to a  
18 variable X, the transform functions for the second set of aliases include a generate  
19 transfer function and a remove transfer function, the generate transfer function  
20 adds the variable X to the second set if the variable Y refers to the same memory  
21 location as one of the aliases in the second set of aliases before the statement, the  
22 remove transfer function removes the variable X.

23  
24      34. The computer-readable medium of claim 23, wherein the type of  
25 statement includes an assignment in which an address of variable Y is assigned to

1 a variable X, the transform functions for the second set of aliases include a  
2 generate transfer function and a remove transfer function, the generate transfer  
3 function is the empty set, the remove transfer function removes the variable X  
4 from the second set.

5

6 35. The computer-readable medium of claim 23, wherein the type of  
7 statement includes a call to a memory allocation function with a return value  
8 assigned to a variable X, the transform functions for the second set of aliases  
9 include a generate transfer function and a remove transfer function, the generate  
10 transfer function is the empty set, the remove transfer function removes the  
11 variable X from the second set.

12

13 36. The computer-readable medium of claim 23, wherein the type of  
14 statement includes an assignment in which a field F pointed to by variable Y is  
15 assigned to a variable X, the transform functions for the second set of aliases  
16 include a generate transfer function and a remove transfer function, the generate  
17 transfer function adds the variable X if the field F pointed to by variable Y refers  
18 to the same memory location as one of the aliases in the second set of aliases  
19 before the statement, the remove transfer function removes the variable X from the  
20 second set of aliases.

21

22 37. The computer-readable medium of claim 23, wherein the type of  
23 statement includes an assignment in which an address of a field F referenced by  
24 variable Y is assigned to variable X, the transform functions for the second set of  
25 aliases include a generate transfer function and a remove transfer function, the

1 generate transfer function is the empty set, the remove transfer function removes  
2 the variable X from the second set.

3

4 38. The computer-readable medium of claim 23, wherein the type of  
5 statement includes an assignment in which a variable Y is assigned to a field F  
6 referenced by variable X, the transform functions for the second set of aliases  
7 include a generate transfer function and a remove transfer function, the generate  
8 transfer function adds the field F referenced by variable X to the second set if the  
9 variable Y refers to the same memory location as one of the aliases in the second  
10 set before the statement, the remove transfer function is the empty set.

11

12 39. The computer-readable medium of claim 23, wherein the transform  
13 functions for the type of statement include a generate transfer function and a  
14 remove transfer function for determining the second set of aliases, the generate  
15 transfer function adds an expression if the expression was updated by the  
16 statement or if one of the memory locations looked up when executing the  
17 statement pointed to a memory location in the second set of aliases, the remove  
18 transfer function is the empty set.

19

20 40. A system for performing path-sensitive value flow analysis on an  
21 abstract program, the abstract program having a plurality of statements that were  
22 derived from complex statements coded within a software program, the system  
23 comprising:

24 a processor; and

1 a memory into which a plurality of instructions are loaded, the plurality of  
2 instructions performing a method comprising:

3 tracking a concrete state and value alias information for each statement  
4 along each relevant path in the abstract program;

5 storing the concrete state and value alias information for each statement  
6 along each relevant path in a symbolic store, the symbolic store storing a plurality  
7 of symbolic states, each symbolic state comprising the concrete state at a specific  
8 location along a specific relevant path in the abstract program, the value alias  
9 information at the specific location along the specific relevant path, the set of  
10 aliases being associated with a designated value that is being analyzed;

11 upon encountering a decisional statement, proceeding individually along  
12 each decision path associated with the decisional statement as long as the concrete  
13 state in the symbolic state at the decisional statement reflects that the decision path  
14 is relevant; and

15 merging two symbolic states in the symbolic store if the two symbolic  
16 states exist for the same specific location in the abstract program and if the value  
17 alias information in the two symbolic states are identical.

18  
19 41. The system of claim 40, wherein the two symbolic states are merged  
20 by deleting information in the concrete state of both symbolic states if the  
21 information differs between the two symbolic states.

22  
23 42. The system of claim 40, wherein the value alias information is  
24 obtained using imprecise memory alias analysis.

1       43. The system of claim 40, wherein the value alias information includes  
2 a first set of aliases that identify aliases for the designated value and a second set  
3 of aliases that identify possible aliases for the designated value.

4  
5       44. The system of claim 43, wherein the second set of aliases is over-  
6 inclusive.

7  
8       45. The system of claim 43, wherein the first set and second set of  
9 aliases are determined by performing transform functions on the first and second  
10 set of aliases based on a type of statement that is being processed in the abstract  
11 program.

12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25